

Notice of Allowability

Application No.

09/458,336

Examiner

Justin T. Darrow

Applicant(s)

GRAVEMAN, RICHARD F.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to an amendment filed 06/30/2004.
2. ☒ The allowed claim(s) is/are 17-20, 22-43, and 45-58.
3. ☒ The drawings filed on 30 June 2004 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
 - * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

DETAILED ACTION

1. Claims 1-65 have been presented for examination. Claims 1-65 have been restricted into Group I, claims 1-16 and 59-65, and Group II, claims 17-58, in an Office action mailed 12/03/2003. Group II, claims 17-58, has been elected without traverse and Group I, claims 1-16 and 59-65, has been withdrawn from consideration in an election filed 03/04/2004. Claims 1-16, 21, 44, and claims 59-65 have been canceled; and claims 17, 35, 38, 40, and 43 have been amended in an amendment filed 06/30/2004. Claims 17-20, 22-43, and 45-58 have been examined.

Election/Restrictions

2. Restriction to one of the following inventions is required under 35 U.S.C. 121:
- I. Claims 1-16 and 59-65, drawn to an approximate message authentication code, a method performed by a cryptography device, and a method for determining an acceptable number of bit differences between a first and second approximate message authentication code, classified in class 714, subclass 758.
 - II. Claims 17-58, drawn to a method performed by a cryptography device and a device for generating an approximate message authentication code, classified in class 713, subclass 168.

The inventions are distinct, each from the other because of the following reasons:

3. Inventions Group II and Group I are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that

Art Unit: 2132

the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because Group II does not recite all the groups of rows do not have the same number of rows. The subcombination has separate utility such as user authentication.

4. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

5. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II, restriction for examination purposes as indicated is proper.

6. A telephone call was made 12/01/2003 to request an oral election to the above restriction requirement, but did not result in an election being made.

7. Applicant's election without traverse of Group II in Paper No. 4, filed 03/02/2004, is acknowledged.

8. Applicant's suggestion of including claims 60-65 in Group II in Paper No. 4, filed 03/02/2004 is acknowledged. The reasoning for this suggestion is on the grounds that the methods in both Group I and Group II are performed on a cryptographic device. This is not found persuasive because the inventions Group I and Group II in combination and subcombination relationship are distinct because (1) the combination as claimed in Group I does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination of Group II has utility by itself or in other combinations (MPEP § 806.05(c)).

The requirement is still deemed proper and is therefore made FINAL.

Drawings

9. The drawings were received on 06/30/2004. These drawings are acceptable.

Allowable Subject Matter

10. Claims 17-20, 22-43, and 45-58 are allowed.

11. The following is an examiner's statement of reasons for allowance:

Claims 17-20, 22-37, and 39; 38; 40-42 and 45-58; and 43 are drawn to two methods and two devices for generating an approximate message authentication code, respectively. The closest prior art, Pires, U.S. Patent No. 6,269,164 B1, discloses similar methods and devices.

Pires illustrates:

receiving a message containing data and arranging the data into a table having $|A|$ columns and T^2 rows, where A and T are integers (see column 13, lines 49-52; figure 15, item 45; receiving sixty-four binary bits of plain text); and

permuting, masking, and copying at least some of the arranged data into T S-arrays, each S-array having $|A|$ columns (see column 14, lines 23-27; figure 12, items 34, 40, and 41; using the Bank by Bank rankings to generate the Mask based on a formula; see column 11, lines 43-46; figures 1, 3, and 4).

However, Pires neither teaches nor suggests determining a majority bit value of each of the $|A|$ columns for each of the T S-arrays, with an odd number of rows. This particular feature incorporated in independent claims 17, 38, 40, and 43 render claims 17-20, 22-37, and 39; 38; 40-42 and 45-58; and 43, respectively, allowable.

Art Unit: 2132

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 until mid October 2004, then (571) 272-3801 thereafter, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830 until mid October 2004, then (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and

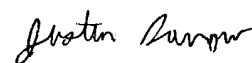
Art Unit: 2132

consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only **"OFFICIAL FAX"** but also **"AMENDMENT AFTER FINAL"**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900 until mid October 2004, then (571) 272-2100 thereafter.

September 17, 2004



**JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100**